IT 인프라 아키텍처 설계

네트워크 고급
VLAN·HA·NAT·LB·GSLB·망분리·NMS

Session 5 · Day 2 — TA의 기업 네트워크 운영 설계 한 권

본문 65 슬라이드 · 강의 시간 약 90분 · TA(Technical Architect) 양성 과정

강사 박수현 · 🚀 젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

왜 네트워크 고급인가 — *국내 통신·NW 장애 3선*

🚫 ① KT 이동통신 장애

2021.10.25 (월)

라우터 설정 변경 중 BGP 오설정 → **전국 KT 유·무선 인터넷 약 89분 마비**.

- 점심 시간 직격 (11:20~12:49)
- 카드결제·증권 거래 전부 영향
- 정부 「통신 장애 보상」 가이드라인 강화

💡 **교훈 — 변경관리(CAB)·롤백 절차·점검 시간대** + 라우팅 검증

> 참고: 「2021 KT 통신장애」 검색

🚫 ② 카카오 5일 장애 (NW 측면)

2022.10.15~10.20

판교 DC 화재 → DNS·LB·세션 동기화 **다중 장애 연쇄**. 메시지·결제·인증 모두.

- DNS TTL 길어 절체 지연
- LB Health Check 미흡
- 세션 복구 → 본인인증·로그인 연쇄 폭주

💡 **교훈 — GSLB·Anycast DNS·LB Health Check·세션 외부화**

> 참고: 「카카오 장애 보고서 과방위」 검색

🚫 ③ 새올 행정망 마비

2023.11.17 (금)

행정안전부 「새올」 인증 인프라 장애 → **전국 민원 시스템 마비** (24시간+).

- L4 LB·인증 서버 NW 경로 문제
- 주민등록·인감 등 발급 불가
- 「공공 NW 이중화 의무」 강화 추진

💡 **교훈 — 공공 NW 이중화·우회 경로·인증 NW 분리**

> 참고: 「2023 새올 행정망 장애」 검색

📌 **이번 세션의 시각** — 위 3건은 모두 **「VRRP/GSLB 미적용」「라우팅 변경 관리 부실」「NW 이중화 부재」**가 핵심. 본 세션의 **VLAN·HA(VRRP)·LB·GSLB·망분리**가 직접 해법.

Session 5 · Day 2 — TA의 기업 네트워크 운영 설계 한 권

세션 5 — *회차 메타데이터*

📋 세션 정보

- **회차**: **5 / 18** — Day 2 · 네트워크 고급
- **소속**: Day 2 — NW 고급 + 스토리지·백업 + 보안 + HA·운영
- **카테고리**: 인프라 고급
- **강의 시간**: 약 90분
- **강사**: 박수현 — 젠아이랩스(GenAI Labs) **CEO / CTO**

🎯 핵심 메시지

> 기초 위에 쌓는 **고급 도구 7종** — **VLAN**으로 분리, **HA/LB**로 살리고, **NAT/QoS**로 다듬고, **망분리/NMS**로 지킨다.

🧭 학습 목표 (Learning Objectives)

1. **VLAN 심화** — Private VLAN·Voice VLAN·VLAN 보안을 설계할 수 있다
2. **STP 보호·스위치 클러스터링** — Stack·vPC·MLAG을 비교 선택한다
3. **HA 프로토콜** — VRRP·HSRP·GLBP·ECMP를 결정 매트릭스로 푼다
4. **NAT·QoS** — NAT 8종·DSCP·CoS·Policing·Shaping을 안다
5. **LB·GSLB** — L4/L7 알고리즘·헬스체크·Persistence·사이트 분산을 설계한다
6. **DHCP·IPv6** — DORA·Option 82·IPv6 주소 체계를 운영자 시각으로 다룬다
7. **망분리·SDN·Overlay·SD-WAN·NMS** — 기업·캠퍼스·WAN을 통째로 본다

PART A

VLAN 심화 — *QinQ · Private VLAN · Voice · VTP · 보안*

> VLAN은 단순히 "방을 나누는 것"을 넘어, QinQ로 ISP·Private VLAN으로 호텔·Voice로 IP전화까지 확장된다.

VLAN 복습 — *Session 4 ↩ 참조 + 심화 진입*

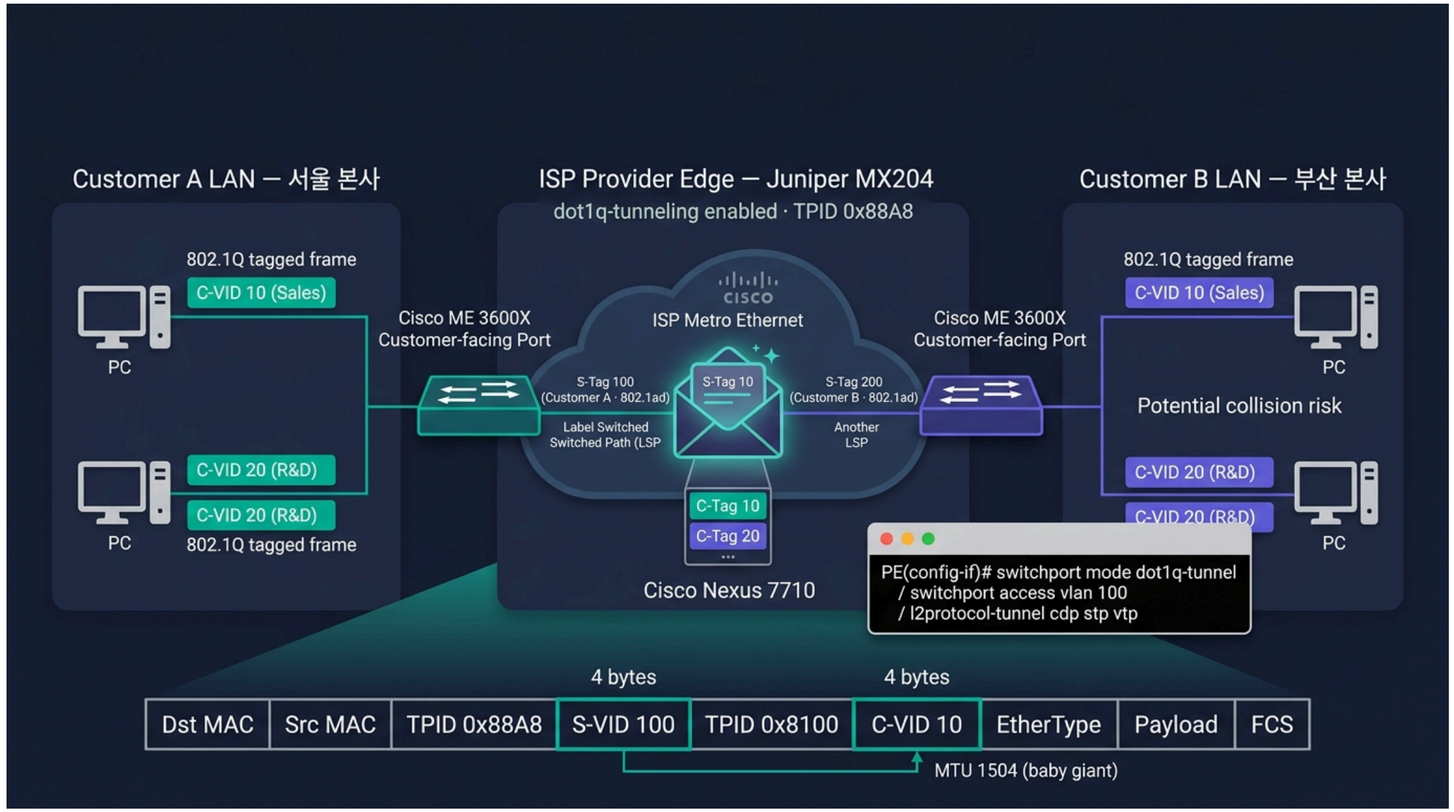
> 🔗 **본문 참조** — VLAN 802.1Q 태깅·Trunk·Access·Native VLAN 본문은 **Session 4** `## VLAN — 802.1Q 태깅` 슬라이드에서 다뤘다. 여기서는 한 줄로 환기만 하고, QinQ·Private VLAN·Voice VLAN·VTP·VLAN 보안으로 곧장 들어간다.

🎯 한 줄 환기

- **VLAN** = L2 broadcast 도메인 격리, 12bit VID = 0~4095 (실용 4,000개)
- **802.1Q 태그** = Ethernet 프레임 안에 4byte 삽입 (TPID `0x8100` + TCI: PCP 3bit / DEI 1bit / **VID 12bit**)
- **Trunk** = 태그 유지하며 SW 간 다중 VLAN 전달, **Access** = 태그 제거 후 단말 전달, **Native VLAN** = Trunk 위의 무태그 1개 (보안상 1번 회피)

🚪 본 세션에서 새로 다루는 것 — Part A의 5장

- **QinQ** (802.1ad) — ISP가 고객 VLAN을 자기 VLAN으로 한 번 더 감싸기
- **Private VLAN** — Primary / Isolated / Community, 같은 서브넷 안에서 단말 격리 (호텔·아파트 패턴)
- **Voice VLAN** — IP 전화 자동 분류, LLDP-MED + CDP 연동
- **VTP** (VLAN Trunking Protocol) — Cisco VLAN DB 자동 동기화, 운영 사고 회피
- **VLAN 보안** — Port Security / DHCP Snooping / DAI / IP Source Guard 액세스 SW 표준 세트



QinQ 다이어그램 (삽화)

Private VLAN — *Primary·Isolated·Community*

🏨 Private VLAN의 동기

- "같은 서브넷 안에서도 단말끼리 통신을 막고 싶다"
- 4094 VLAN을 잡아먹지 않고 격리 — VLAN 1개 안에서 sub-격리

🎯 3종 VLAN

종류	통신 가능 대상
Primary	모든 Secondary와 + 외부
Isolated (격리)	**Primary와만** — 동일 Isolated끼리도 차단
Community (공동체)	**같은 Community 내부 + Primary** — 다른 Community 차단

🚪 Port Type

- **Promiscuous Port** — Primary VLAN에 연결, 모든 단말과 통신 (라우터·GW용)
- **Isolated Port** — Isolated VLAN, 다른 단말과 단절
- **Community Port** — 같은 Community 내부만 가능

🏢 활용 시나리오

- **호텔 객실** — 객실끼리 차단(Isolated), 공용 GW로만
- **공공 와이파이** — 사용자 간 격리
- **DC 멀티테넌트** — 고객 그룹 분리
- **DMZ 서버 분리** — 서로 침투 차단

PART C

STP·스위치 클러스터링 — *Stack·vPC·MLAG*

> STP는 보호되어야 한다. 그리고 STP를 우회해서 진짜 Active-Active를 만드는 도구가 클러스터링이다.

BPDU Guard / Root Guard / Loop Guard

🛡️ BPDU Guard

- **Edge (PortFast) 포트에 BPDU 수신 시 → 즉시 Err-Disable**
- 사용자가 무단으로 스위치를 액세스 포트에 꽂는 사고 차단
- **모든 액세스 포트의 표준 설정**

```
spanning-tree portfast edge default
spanning-tree portfast bpduguard default
```

🛡️ Root Guard

- "이 포트는 절대 Root 방향이 아니다"
- 이 포트에서 **Superior BPDU** 수신 → **Root Inconsistent** 상태 (Forwarding 중단)
- 운영자 의도 외의 Root 선출 차단 — **코어 SW의 다운링크에 적용**

🛡️ Loop Guard

- 단방향 링크 또는 BPDU 손실로 인한 잘못된 Forwarding 차단
- BPDU 안 받으면 → **Loop Inconsistent** 상태로 차단
- Trunk 포트에 적용

🎙️ TA 매트릭스

위치	권장
액세스 포트	PortFast + BPDU Guard + Port Security
코어 다운링크	Root Guard
광 Trunk	Loop Guard

스위치 Stacking — *Cisco StackWise · HPE IRF · Aruba VSF*

🧩 Stacking이란

- 여러 물리 스위치를 **하나의 논리 SW** 로 묶음
- 백플레인급 Stack Cable로 연결
- **단일 IP·단일 설정·단일 관리 평면**
- LAG/LACP을 여러 SW 멤버에 걸쳐 구성 가능 (실질적 MLAG)

🏭 벤더별 명칭

벤더	명칭
Cisco	**StackWise / StackWise Virtual**
HPE	**IRF (Intelligent Resilient Framework)**
Aruba	**VSF (Virtual Switching Framework)**
Juniper	**Virtual Chassis (VC)**
Arista	(별도 — MLAG 선호)

⚖️ 장점·단점

장점	단점
단일 관리	펌웨어 업그레이드 시 전체 영향 가능
LAG/MLAG 자연스러움	Stack Cable 장애 = 분할(Split) 위험
구성 단순	Stack 멤버 수 한계 (보통 4~9대)
액세스 SW에 인기	코어/Spine에는 부적합

🎙️ TA 권고

- **액세스/집선 = Stacking 권고**
- **코어/Spine = vPC/MLAG 권고** (펌업 시 분리 가능)
- Stack 멤버는 **동일 모델 + 동일 IOS** 권고

PART D

HA 프로토콜 — *VRRP · HSRP · GLBP · ECMP*

> 게이트웨이 한 대만 죽어도 전체가 멈춘다. 표준 답은 가상 IP를 둘이서 나눠 갖는 것.

VRRP (Virtual Router Redundancy Protocol) — *RFC 5798*

🎯 VRRP 동작

- **2~N대의 라우터가 가상 IP/MAC** 을 공유
- **Master 1대**가 가상 IP를 응답 — 나머지는 Backup
- Master가 1초마다 Advertisement 보냄
- Backup이 3.6초간 못 받으면 → **새 Master 선출**
- 단말은 **가상 IP만 게이트웨이로 알면 됨**

🏗️ Master 선출

- 가장 높은 **Priority** (0~255, 기본 100)
- Owner (실IP=가상IP) = **Priority 255** (자동 Master)
- 동률이면 **IP 큰 쪽**

🔌 Virtual MAC

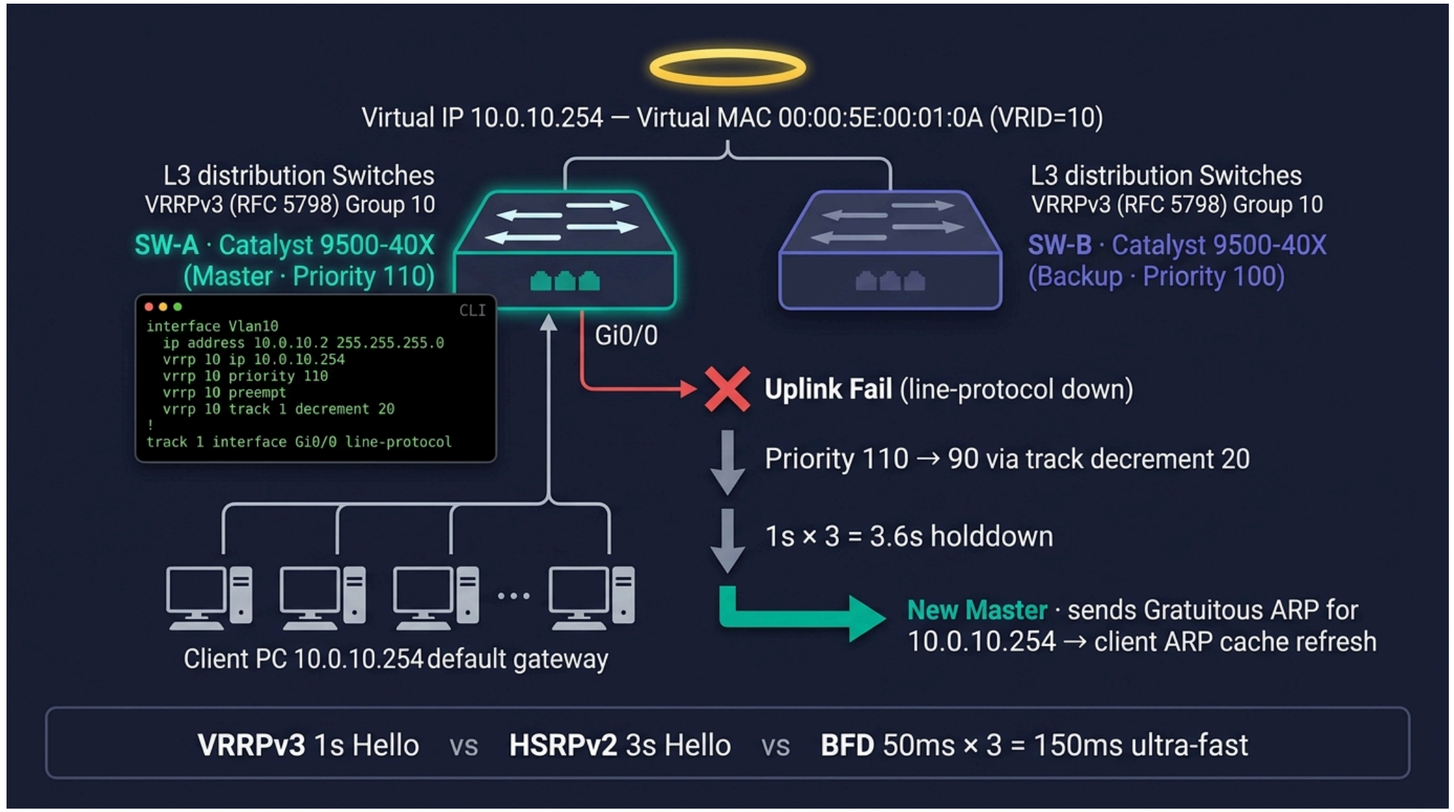
- IPv4: `00:00:5E:00:01:VRID`
- VRID = VRRP Group ID (1~255)
- 절체 시 새 Master가 **Gratuitous ARP** 발송 → 단말 ARP 캐시 갱신

🛰️ Tracking

- 업링크 인터페이스 또는 라우트가 **down** 되면 Priority 자동 감소
- → 자동 절체 유발
- 예: 업링크 다운 → Priority 110 → 100 → 다른 SW가 Master

🎙️ TA 메모

- VRRPv3 (RFC 5798) = **IPv4 + IPv6** 동시 지원
- VRRPv2 = IPv4 only
- 벤더 중립 — Cisco·Juniper·Arista·HPE 모두 지원



VRRP 동작 (삽화)

HSRP · GLBP · CARP — *VRRP의 변종*

프로토콜	표준	벤더	특징
VRRP	**RFC 5798**	표준	Master 1대, Active-Standby
HSRP	RFC 2281 (info)	**Cisco 독자**	Active 1대 + Standby 1대, Hello 3초
GLBP	(Cisco 독자)	Cisco	**Active-Active** — 가상 MAC 여러 개를 단말에 분배
CARP	OpenBSD	BSD 진영	VRRP 호환, BSD/pfSense

🔵 HSRP 핵심

- Group: 0~255 (v1) / 0~4095 (v2)
- Virtual MAC: `00:00:0C:07:AC:GG`
- States: Init → Listen → Speak → Standby → Active
- Hello 3초, Hold 10초 (기본)
- Tracking 지원

🟢 GLBP 핵심

- AVG (Active Virtual Gateway) — 가상 IP의 ARP 응답 담당
- AVF (Active Virtual Forwarder) — 가상 MAC별 포워딩
- **단말 그룹별로 다른 MAC** 반환 → Active-Active 부하 분산
- Cisco 독자

🎯 결정 매트릭스 — VRRP vs HSRP

항목	VRRP	HSRP
표준	**IETF RFC**	Cisco 독자
멀티벤더	⭕	△ (Cisco only)
IPv6	v3 지원	가능
Hello	1초	3초
절체 시간	3.6초	10초
운영자 인지도	신규 표준	한국 SI 현장 압도적

🎙️ 권고

- **신규 사업 = VRRP**
- 기존 Cisco 단독 사이트 = HSRP 잔존 OK
- Active-Active = GLBP 또는 MLAG

VRRP·HSRP 콘솔 — *Cisco IOS 실제 설정*

```
! ──────── VRRP (RFC 5798) — SW-A: Master ────────
SW-A# configure terminal
SW-A(config)# interface Vlan10
SW-A(config-if)#  ip address 10.0.10.2  255.255.255.0
SW-A(config-if)#  vrrp 10 ip 10.0.10.1               ! Virtual IP
SW-A(config-if)#  vrrp 10 priority 110               ! 더 큼 = Master
SW-A(config-if)#  vrrp 10 preempt
SW-A(config-if)#  vrrp 10 authentication md5 key-string  Sup3rS3cret
SW-A(config-if)#  vrrp 10 timers advertise 1         ! Hello 1s
SW-A(config-if)#  vrrp 10 track 1 decrement 20       ! 업링크 다운 시 -20
SW-A(config-if)# exit

SW-A(config)# track 1 interface GigabitEthernet0/0  line-protocol
SW-A(config)# end

! ──────── VRRP — SW-B: Backup (priority 100) ────────
SW-B(config-if)# vrrp 10 ip 10.0.10.1
SW-B(config-if)# vrrp 10 priority 100

! ──────── HSRP (Cisco 독자) ────────
SW-A(config-if)# standby version 2
SW-A(config-if)# standby 10 ip 10.0.10.1
SW-A(config-if)# standby 10 priority 110
SW-A(config-if)# standby 10 preempt
SW-A(config-if)# standby 10 timers msec 200 msec 750  ! 빠른 절체
SW-A(config-if)# standby 10 track 1 decrement 20
```

TA 표준 세트: `preempt` + `track` + `timers msec` + 인증. 절체 시 GARP가 흐름. 신규 = VRRP, 잔존 Cisco-only = HSRP.

ECMP (Equal-Cost Multi-Path) — *동일 비용 다중 경로*

🛤️ ECMP 개념

- 같은 목적지로 **비용이 동일한 N개 경로**가 있을 때
- 라우터가 **N개 모두에 트래픽을 분산**
- **Active-Active 라우팅**
- Spine-Leaf DC의 표준 동작

🎲 해시 알고리즘

- **L3 Hash**: Src IP + Dst IP
- **L4 Hash**: + Src/Dst Port (Per-Flow)
- **Polarization 회피** — 동일 해시 키 사용 시 분기점마다 같은 경로 선택 → 일부 링크 과부하

🔢 Per-Packet vs Per-Flow

모드	장점	단점
Per-Packet	균등 분산	**재정렬** → TCP 성능 ↓
Per-Flow ⭐	같은 플로우는 같은 경로	큰 플로우는 한 링크에 집중

🎯 라우팅 프로토콜 지원

- OSPF/IS-IS — 동일 cost 자동 ECMP
- BGP — `maximum-paths` 설정 + AS-PATH 동일 조건
- 일반 라우터 = 최대 4·8·16·32·64 경로

🎙️ TA 메모

- DC Spine 대역폭 확장의 표준 도구
- BGP EVPN-VXLAN과 결합

PART E

NAT·QoS — *주소 변환 8종 · 큐잉 정책*

> 외부와 내부의 경계에서는 주소를 바꾸고, 트래픽의 종류에 따라 줄을 세운다.

NAT 종류 — *8가지 변형*

종류	동작	주 용도
Static NAT (1:1)	내부 IP ↔ 외부 IP 고정	서버 공개 (웹·메일)
Dynamic NAT	내부 IP → 풀의 외부 IP 임시 매핑	다수 내부 사용자
PAT (NAPT) ⭐	다수 내부 IP → 1개 외부 IP + 포트 변환	**가정·기업 인터넷 표준**
Hairpin NAT (NAT Loopback)	내부 → 외부 공인IP로 접근 시 다시 내부로	내부에서 자사 웹 접속
Twice NAT (Bidirectional)	Src·Dst 모두 변환	사이트 간 IP 충돌 해결
NAT64	IPv6 ↔ IPv4 양방향	IPv6 단말이 IPv4 서버 접근
NAT46	IPv4 → IPv6	드물게
CGN (LSN)	통신사 대규모 PAT	IPv4 고갈 대응

현장 단순화: 가정/사무실 = **PAT**, 서버 공개 = **Static**, IPv6 전환 = **NAT64**, 통신사 = **CGN**.

NAT 보안 · NAT-Traversal — *STUN · TURN · ICE*

🔒 NAT의 보안 효과 (부수적)

- 내부 사설 IP가 외부에 노출 안 됨
- 외부에서 직접 connect 불가 (Static 제외)
- **단, NAT 자체는 보안 솔루션이 아님** — FW가 별도 필요

⚠️ NAT의 부작용

- **End-to-End 깨짐** — IPsec AH 호환 안 됨 (ESP는 NAT-T 필요)
- VoIP·P2P 어려움
- 로그·감사 추적 복잡 (외부에서 보면 1 IP)
- Active FTP·SIP·H.323 → ALG (Application Layer Gateway) 필요

🌐 NAT-Traversal 기술

- **STUN** (RFC 5389) — 자신의 공인 IP·포트 발견
- **TURN** (RFC 8656) — 중계 서버 경유 (STUN 실패 시)
- **ICE** (RFC 8445) — STUN+TURN 후보 자동 선정
- **WebRTC** 의 표준 백본

🛠️ 운영 관점

- VoIP·화상회의·게임·원격제어 = STUN/TURN
- **IPsec NAT-T (UDP 4500)** — VPN을 NAT 너머로
- 기업 FW는 SIP·H.323 ALG 동작 정책 점검 필수

QoS 큐잉 — *DSCP · CoS · 우선순위 표시*

🏷️ 표시 (Marking)

- **CoS (802.1p)** — L2, VLAN 태그의 PCP 3bit (0~7)
- **DSCP** — L3, IP TOS의 6bit (0~63), 64개 클래스
- **MPLS EXP** — MPLS 라벨의 3bit

🎯 DSCP 클래스

클래스	DSCP	용도
EF (Expedited Forwarding)	46	음성 (VoIP)
AF41	34	영상 회의
AF31	26	영상 스트리밍
AF21	18	트랜잭션
CS6	48	라우팅 제어 (OSPF·BGP)
CS0 (BE)	0	Best Effort (기본)

🎭 분류 (Classification)

- DSCP·CoS 신뢰 (Trust) — Edge가 이미 표시했다면 신뢰
- ACL 매칭 — 출발/도착 IP/Port로 분류
- NBAR (Cisco) — 응용 시그니처로 분류

🚦 큐잉 알고리즘

알고리즘	특징
FIFO	단일 큐, 우선순위 없음
WFQ (Weighted Fair Queue)	플로우별 공평 분배
CBWFQ (Clas6-Based)	클래스별 대역폭 보장
LLQ (Low Latency Queue) ⭐	CBWFQ + PQ → **VoIP 표준**

🎙️ TA 메모

- VoIP·영상 = LLQ + 명시적 대역폭
- 데이터는 CBWFQ 클래스로 분배

Policing vs Shaping — *드롭 vs 지연*

🚓 Policing

- 정해진 속도 초과분을 **즉시 드롭** (또는 Remark)
- **Inbound** 적용이 일반
- Token Bucket 알고리즘
- 빠르고 단순, 저메모리

📉 단점

- TCP 재전송 폭주 가능
- 사용자 체감 품질 저하

🌊 Shaping

- 초과분을 **버퍼에 저장**했다가 천천히 보냄
- **Outbound** 적용이 일반
- Leaky Bucket / Token Bucket
- 메모리·지연 증가

📈 장점

- 평활한 트래픽
- TCP 친화적

🎯 결정

상황	권고
ISP 가입자 초과 단속	Policing
WAN 회선 한계 맞춤 송출	**Shaping**
QoS Marking	Policing의 Remark 활용

VoIP·영상회의 QoS 정책 — *현장 표준 설정*

🎙️ VoIP 요구사항

- **One-way Latency** < 150ms
- **Jitter** < 30ms
- **Loss** < 1%
- 대역 = G.711(80kbps) / G.729(24kbps) per call
- BFCP·SIP 시그널링은 별도 우선순위

📹 영상회의 요구사항

- HD = 2~4 Mbps
- 4K = 8~15 Mbps
- Loss < 0.5%
- 같은 LLQ 그룹 또는 별도 AF41

🎯 표준 정책 (예)

트래픽	표시	큐	대역
Voice RTP	EF (46)	**LLQ**	회선의 10~33% (한도)
Voice 시그널링 (SIP)	CS3 (24)	CBWFQ	작게
Video	AF41 (34)	CBWFQ	25%
Mission Critical Data	AF31 (26)	CBWFQ	25%
Best Effort	CS0 (0)	CBWFQ default	나머지
Scavenger (백업·P2P)	CS1 (8)	WRED 일찍 드롭	잔여

🎙️ TA 메모

- LLQ 한도는 회선의 **33% 이하** 권고
- WAN 회선 = Shaping으로 ISP 약정 속도에 맞춤

PART F

로드 밸런싱 — *L4 · L7 · 알고리즘 · 솔루션*

> 단일 서버는 한계가 있다. 여러 서버 앞에 LB를 두면 가용성·확장성·보안 모두 얻는다.

L4 vs L7 — *결정의 첫 갈래길*

⚙️ L4 LB (Transport)

- **5-Tuple** 보고 분배 (Src IP·Src Port·Dst IP·Dst Port·Protocol)
- 페이로드 무관 — HTTP·HTTPS·DB·SMTP 등 모든 TCP/UDP
- **빠름·저오버헤드** — 수십만 cps
- DSR(Direct Server Return) 가능
- L4 표준 솔루션 = LVS · HAProxy(TCP 모드) · F5(LTM L4)

🎯 사용 사례

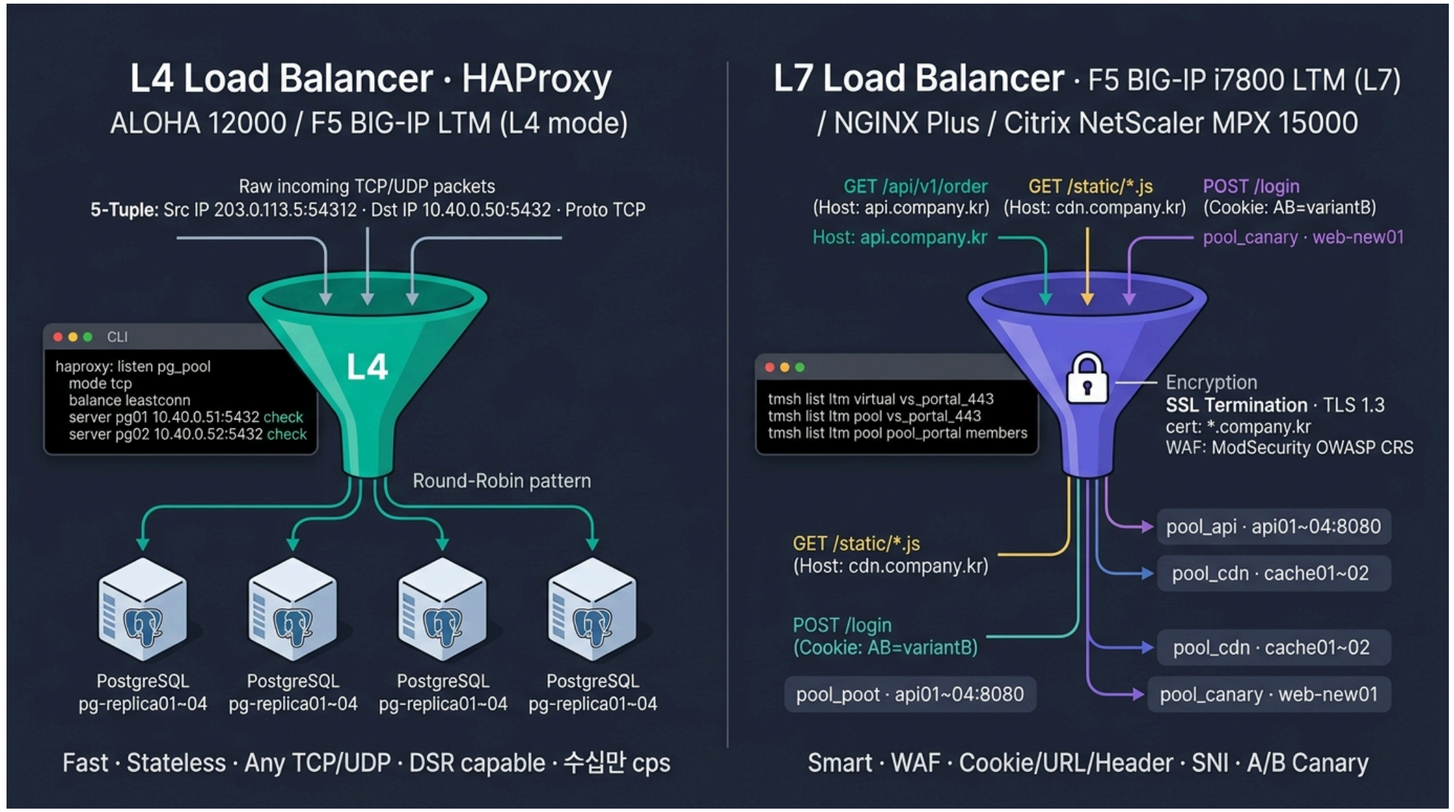
- DB 클러스터 (3306·5432·1521)
- TCP 응용 (SMTP·LDAP·RDP)
- 단순 HTTP 부하 분산

🌐 L7 LB (Application)

- HTTP/HTTPS/gRPC 등 **응용 페이로드** 분석
- **URL·Header·Cookie·Method** 보고 분배
- SSL Termination → 백엔드는 평문
- WAF·Rate Limit·인증·Caching 부가 기능
- L7 표준 = NGINX · HAProxy · F5 LTM(L7) · Citrix NetScaler

🎯 사용 사례

- `/api` → **API 서버,** `/static` → **캐시**
- **A/B 테스트** (Header·Cookie 기반)
- **Canary 배포** (가중치)
- 다중 도메인 → 단일 IP



L4 vs L7 (삽화)

L4 LB 알고리즘 — *분배 방식*

알고리즘	동작	적합
Round Robin (RR)	순서대로 1→2→3→1	균등한 서버
Weighted RR	가중치 비율 (2:1:1)	사양 다른 서버
Least Connections ⭐	현재 활성 연결 최소 서버	**세션 긴 서비스 (DB·WebSocket)**
Weighted Least Conn	가중치 + 연결 수	세션 + 사양 차이
IP Hash (Source Hash)	Src IP 해시로 고정 매핑	Session Persistence 대안
URL Hash (L7)	URL 해시	캐시 친화
Random	임의	단순
Least Response Time	응답시간 가장 빠른 서버	가용성 보장 안되면 위험

한 줄 결정: 짧은 요청 = **RR/WRR**, 긴 세션 = **Least Conn**, 캐시 = **URL/IP Hash**.

L7 LB — *URL·Header·Cookie·SSL Termination*

🎯 L7 컨텐츠 스위칭

- **Path 기반**: `/api/*` → API 백엔드, `/static/*` → CDN
- **Host Header**: `www.a.com` → A 풀, `www.b.com` → B 풀
- **HTTP Method**: GET → 캐시, POST → 직접 백엔드
- **Cookie**: A/B 테스트 그룹 분기
- **User-Agent**: 모바일 vs 데스크톱
- **Geo IP**: 국가별 다른 풀

🔐 SSL Termination

- LB에서 TLS 종단 → 백엔드는 평문 HTTP
- 인증서 관리 1곳 (LB)
- 백엔드 CPU 절감
- 단점: 내부 평문 → DC 내부망 보안 신뢰 필요

🔐 SSL Bridging (Re-encrypt)

- LB가 TLS 종단 → 백엔드 TLS 재암호화
- WAF·정책 적용 + 내부 암호 유지
- 더 안전, CPU 더 씀

🔐 SSL Pas6-through

- LB가 SNI만 보고 라우팅 → TLS 그대로 백엔드
- WAF·L7 정책 불가
- 가장 단순

🎙️ TA 메모

- 일반: **SSL Termination + WAF**
- 금융·의료: **SSL Bridging**
- gRPC mTLS 또는 SSH = Pas6-through

헬스 체크 — *Active vs Passive*

🩺 Active Health Check

- LB가 주기적으로 **테스트 요청** (HTTP GET /health)
- 응답 시간·상태 코드·콘텐츠 검증
- 실패 N회 → 풀에서 제외 (Drain)
- 복구 M회 → 다시 투입
- 간격: 보통 5~30초

🩺 Passive Health Check

- 실제 클라이언트 요청 응답을 모니터링
- 5xx·Timeout 발생 시 풀에서 제외
- 즉시성 ↑, 가짜 양성 ↑

🎯 헬스 체크 종류

레벨	검사	비고
ICMP Ping	L3 응답	가장 단순, 응용 무관
TCP Connect	3-way 성공	L4 표준
HTTP GET /health	200 OK + 응답 본문	**L7 표준** ⭐
TLS Handshake	인증서 유효성	HTTPS 서비스
Script (gRPC·DB·Custom)	응용 종속	정확도 ↑

🎙️ TA 메모

- **/health 엔드포인트는 응용 + DB까지 점검**해야 의미
- 단순 200 OK는 "프로세스 살았다" 만 의미

Session Persistence — *Sticky Session*

🔗 왜 필요한가

- 세션 정보가 서버 메모리에 있을 때 — 다른 서버로 가면 로그아웃
- 장바구니·로그인 상태·WebSocket
- 외부 세션 스토어(Redis)를 쓰지 않는 응용

🎯 Persistence 방식

방식	동작	단점
Source IP	클라이언트 IP 해시	NAT 뒤 다수 사용자 한 서버 집중
Cookie Insert ⭐	LB가 쿠키 발급	HTTP/HTTPS 한정
App Cookie Learn	서버가 발급한 쿠키 학습	응용 의존
SSL Session ID	TLS 재사용 키	TLS 1.3에서 변경
Header (X-Forwarded)	임의 헤더	응용 협조 필요

⚠️ Persistence의 부작용

- **부하 불균형** — 일부 서버에 트래픽 집중
- **장애 시 세션 손실** — 그 서버만 죽으면 그 세션도 끝
- 외부 세션 스토어(Redis·DB)가 진짜 해법

🎙️ TA 권고

- **무상태 응용 + Redis 세션 스토어** = 최고
- 어쩔 수 없으면 Cookie Insert
- Source IP는 모바일 캐리어 NAT 환경 부적합

LB 솔루션 비교 — *F5 · Citrix · A10 · HAProxy · NGINX · KEMP · Radware*

솔루션	형태	강점	일반 사용
F5 BIG-IP LTM	하드웨어/가상	**시장 1위**, iRules 강력, WAF(ASM)·DNS(GTM) 연계	**국내 대기업·금융 표준**
Citrix NetScaler (NetScaler ADC)	하드웨어/가상	App Delivery + AAA·WAF, Citrix VDI 연계	VDI 환경
A10 Thunder	하드웨어/가상	가성비, CGN·DDoS 우수	통신사·중견기업
Radware Alteon	하드웨어/가상	DDoS·SSL 강점	보안 강조
HAProxy	SW (OSS+상용)	**고성능·경량·세밀 제어**	**MSA·DC 내부**
NGINX / NGINX Plus	SW (OSS+상용)	웹서버 + LB + Caching	웹·API GW
KEMP LoadMaster	SW/하드웨어	중소규모 가성비, Exchange 친화	중소·MS 스택
AVI Networks (VMware NSX ALB)	SW Defined	DC SDN 통합	NSX 환경
클라우드 LB	관리형	AWS ALB/NLB·Azure LB·GCP LB·NCP LB	클라우드
K8s Ingress / Service Mesh	SW (OSS)	NGINX·Traefik·Istio·Contour·HAProxy·Envoy	MSA·컨테이너

한국 현장 단순화 — 금융·공공 대기업 = **F5**, 통신사 = A10/Radware, 신규 MSA = **HAProxy/NGINX**, VDI = NetScaler, K8s = NGINX Ingress·Istio.

> 📷 **실제 장비·UI 참조** (벤더 공식) - F5 BIG-IP rSeries Hardware — F5 공식 - F5 BIG-IP Configuration Utility (TMUI) / iControl REST — F5 TechDocs (관리 UI) - Citrix NetScaler ADC — NetScaler 공식 - A10 Thunder ADC — A10 공식 - Radware Alteon — Radware 공식 - HAProxy Enterprise Console — HAProxy 공식

PART G

GSLB — *Global Server Load Balancing · 사이트 간 분산*

> 한 LB로 단일 사이트, GSLB로 여러 사이트·국가 분산이 가능해진다.

GSLB — *왜 필요한가*

🌍 GSLB가 푸는 문제

- 단일 LB로는 **단일 DC** 만 보호 — DC 통째 장애 시 모두 마비
- 글로벌 서비스에서 **사용자 가까운 사이트** 로 자동 라우팅 필요
- DR 시 **자동 DNS 절체** 필요 — 수동 변경 = 24~48시간 TTL

🎯 GSLB의 3가지 결정

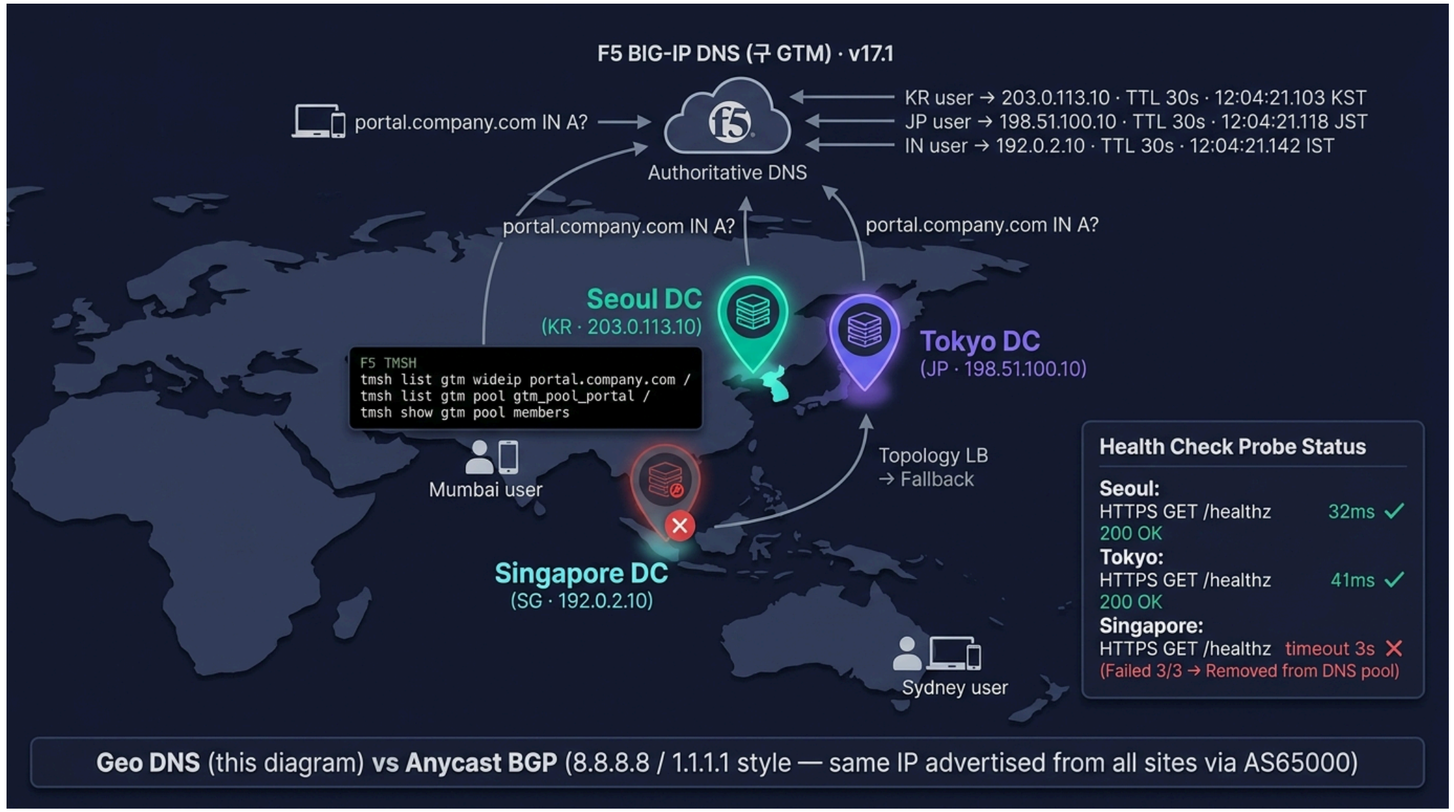
1. **헬스** — 어느 사이트가 살아있나
2. **위치** — 사용자에게 가까운 사이트
3. **부하** — 어느 사이트의 LB가 여유 있나 → 종합해서 **DNS 응답으로 IP를 다르게** 반환

🛠️ 구현 방식

- **DNS 기반** (가장 흔함) — 도메인 질의에 위치/헬스에 따라 다른 A 레코드 반환
- **Anycast 기반** — 같은 IP를 여러 사이트가 BGP 광고, 라우팅이 최단 사이트로
- **HTTP Redirect** — L7에서 302로 위치 변경 (구식)

🎙️ TA 메모

- 한국 공공 단일국가 서비스도 **DR 자동 절체**용으로 GSLB 도입 일반화
- TTL을 짧게 (30~60초) 유지하는 것이 절체 시간 단축



GSLB 다이어그램 (삽화)

헬스체크 · Active-Active · DR Failover

🩺 GSLB 헬스 체크

- **ICMP Ping** — 가장 단순, 응용 무관
- **TCP Connect** — 포트 열림 여부
- **HTTP GET /health** — 응용 레벨
- **Scripted** — 특정 응답·DB 쿼리
- 보통 사이트당 **여러 종류 동시** 검사
- 주기 30초·실패 3회 = 90초 절체

🌐 사이트 모드

모드	특징
Active-Active	모든 사이트 동시 가동, 사용자 분산
Active-Standby	메인 사이트 우선, 장애 시만 보조
Weighted	가중치로 비율 분배 (Canary·신규 DC)

🚨 DR Failover 시나리오

1. 메인 DC HTTP 헬스체크 실패
2. GSLB가 DR DC IP 반환 시작
3. 짧은 TTL(30~60초)에 따라 단말 DNS 캐시 만료
4. 새 요청은 DR DC로 → **2~5분 내 90% 절체**

🎙️ TA 권고

- **DR 사이트 사전 가동** (Warm/Hot) 권고 — Cold면 부팅 시간 추가
- 데이터 복제 RPO와 GSLB TTL 정합 확인
- **반기 1회 GSLB Failover 훈련** (Tabletop or 실제)

GSLB 솔루션 — *F5 DNS · Citrix ITM · Akamai · Route 53*

솔루션	형태	강점	일반 사용
F5 DNS (구 GTM)	어플라이언스/가상	LTM과 통합·iQuery로 LB 부하 인지	**국내 대기업 표준**
Citrix ITM (NetScaler GSLB)	어플라이언스	NetScaler 환경	VDI 사이트
A10 Thunder GSLB	어플라이언스	가성비	통신사
Infoblox NIOS DTC	DDI 통합	IPAM·DHCP·DNS 통합	대기업
Akamai GTM	글로벌 SaaS	글로벌 PoP, 분석	글로벌 서비스
AWS Route 53	클라우드	Health Check·Geo·Weighted·Failover	클라우드
Azure Traffic Manager	클라우드	Performance·Priority·Weighted	Azure
Cloudflare Load Balancing	글로벌 SaaS	빠른 절체·Anycast	글로벌 SaaS
NS1 / NS-One	글로벌 SaaS	데이터 기반 라우팅	핀테크

PART H

DHCP · Multicast · IPv6 — *주소·그룹·전환*

> 자동 주소 할당, 그룹 통신, 차세대 주소 — 세 가지 핵심 인프라.

DHCP 복습 — *Session 4 ↩ 참조 (DORA · Option · Snooping)*

> 🔗 **본문 참조** — DHCP DORA 4단계 흐름·Relay·Option 표·Snooping 보안은 **Session 4** `## DHCP — DORA 4단계` 슬라이드에서 본문급으로 다뤘다. 여기서는 한 줄 환기만 하고 망분리·DNS·QoS 로 진입한다.

🎯 한 줄 환기

- **DHCP** = IP·서브넷·GW·DNS·NTP 를 단말에 자동 분배 (수동 정적 IP 의 표준 대안)
- **DORA 4단계** = **D**iscover (Broadcast) → **O**ffer → **R**equest (Broadcast) → **A**ck, 같은 서브넷 한정 — 다른 서브넷은 **Relay (Option 82)**
- **자주 쓰는 옵션** = 1 (Mask) · 3 (GW) · 6 (DNS) · 15 (Domain) · 42 (NTP) · 43 (Vendor, AP Controller 자동 발견) · 51 (Lease) · 82 (Relay 정보) · 150 (IP Phone TFTP)
- **Lease 갱신** = T1 (50%) Unicast → T2 (87.5%) Broadcast → 만료 시 DORA 재시작
- **액세스 SW 보안 표준 세트** = **DHCP Snooping** (위조 서버 차단) + **DAI** (ARP 위조 차단) + **IP Source Guard** (Snooping 바인딩 외 차단)

PART I

망분리 · DMZ — *물리·논리 분리, KISA 가이드*

> 한국 공공·금융의 핵심 보안 요건. 인터넷망·업무망을 어떻게 나누는가가 설계의 절반.

망분리 개요 — *왜·무엇을 분리하는가*

🛡️ 망분리의 목적

- **인터넷 위협 차단** — 악성코드·랜섬웨어
- **개인정보 유출 방지** — 업무망 데이터가 인터넷으로 못 가게
- **법령 준수** — 정보통신망법·개인정보보호법·금융업 감독규정
- KISA 망분리 가이드(2013~) — 공공·금융 의무

🎯 분리 대상

- **인터넷망** — 외부 통신, 웹 브라우징, 메일 일부
- **업무망 (내부망)** — 사내 시스템, 개인정보, 핵심 자료
- 일부는 **개발망·운영망·DMZ** 까지 추가 분리

🚪 2가지 큰 방식

방식	특징
물리적 망분리	별도 PC·별도 NIC·별도 케이블·별도 SW
논리적 망분리	1대 PC·1대 SW + 가상화·VLAN·VDI로 격리

🎙️ TA 메모

- 금융권 = **물리적 망분리 기본** (전자금융감독규정)
- 공공 = 물리 또는 논리 (조직별)
- 일반 기업 = 논리 + DLP·EDR

물리적 망분리 — *2PC · 공용 PC · 전용 NIC*

💻 2 PC 방식

- 인터넷용 PC + 업무용 PC를 **각각 별도**
- 사용자 책상에 2대
- KVM 스위치로 모니터·키보드 공유 가능
- **가장 강한 분리, 가장 비싼 구축**

💻 공용 PC + 2 NIC

- 1대 PC, NIC 2장
- 사용자가 부팅 시 또는 SW로 모드 전환
- 동시 사용 불가
- 중간 보안 수준

🔌 전용 NIC + VLAN

- 1대 PC, NIC 2장 동시 운영 (인터넷 + 업무)
- 각 NIC가 다른 VLAN·다른 SW에 연결
- OS 라우팅 정책으로 트래픽 분리
- **편의성 ↑, 보안 ↓** (악성코드 한 OS에서 양쪽 접근 가능)

🎙️ TA 결정

- **금융 = 2PC 또는 가상화 망분리(VDI)**
- 공공 = 2PC 또는 SBC(Server-Based VDI)
- 일반 기업 = 1PC + VDI 가상 환경

논리적 망분리 — *SBC · CBC · VDI*

🖥️ SBC (Server-Based Computing)

- **응용/세션을 서버에서 실행**, 화면만 사용자 PC로 (RDP/ICA/HDX)
- 인터넷 영역을 서버 팜에 격리
- 사용자 PC = 단순 뷰어
- Citrix Virtual Apps and Desktops, Microsoft RDS

🖥️ CBC (Client-Based Computing)

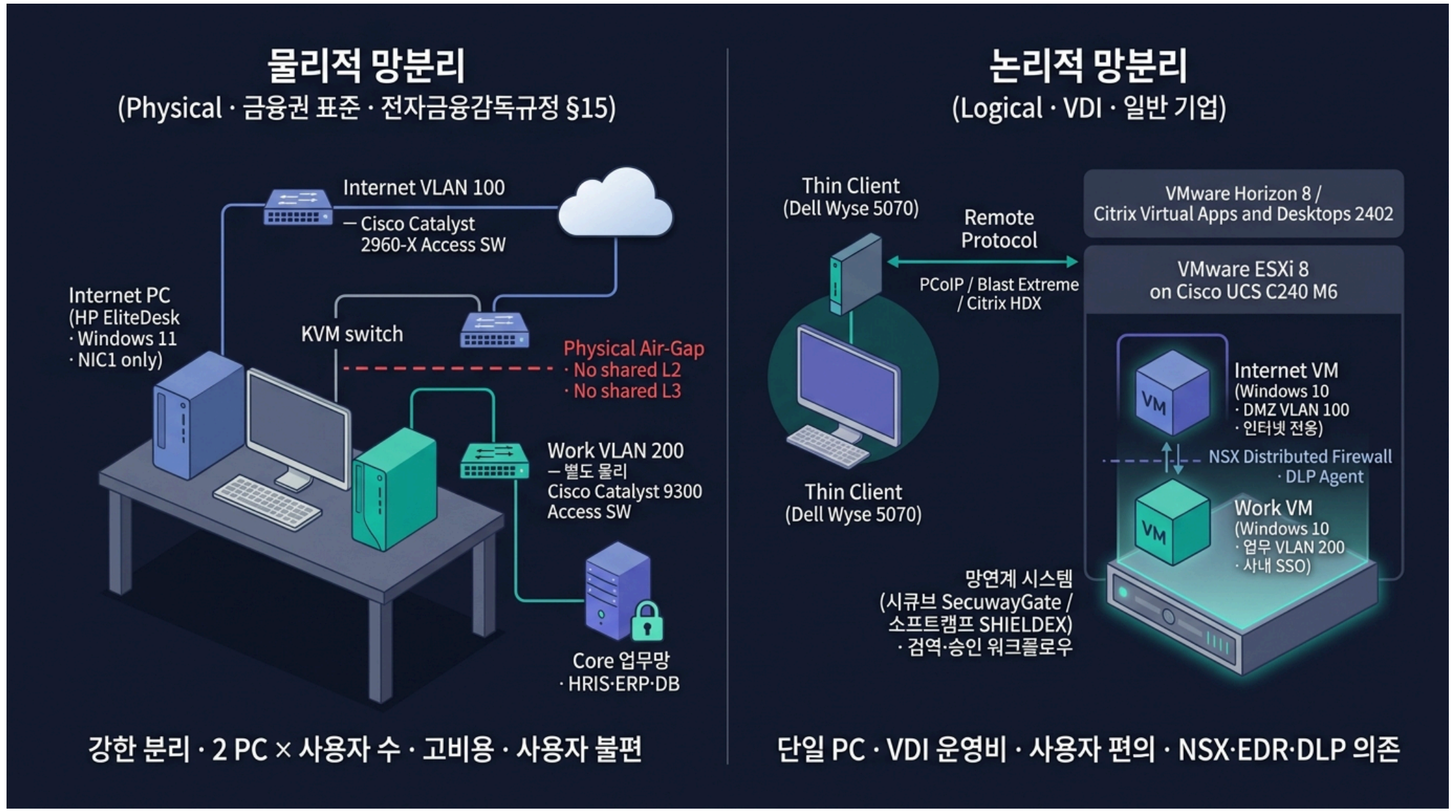
- 사용자 PC의 **로컬 가상머신(VM/컨테이너)** 으로 분리
- 한 PC 안에 인터넷용 가상 OS 별도
- 망간 자료 전송 제어
- 사례: 안랩, 시큐브 등 국내 솔루션

🖼️ VDI (Virtual Desktop Infrastructure)

- 사용자별 **개인 가상 데스크톱**을 DC에서 운영
- 사용자 PC는 Thin Client 또는 일반 PC + 클라이언트
- VMware Horizon · Citrix Virtual Desktops · Azure Virtual Desktop
- **인터넷용 VDI + 업무용 PC** 조합으로 망분리

🎙️ TA 메모

- 신규 사업 = **VDI 기반 논리 망분리** 증가
- 5G/재택근무로 **DaaS** (Desktop as a Service) 도 검토



망분리 비교 (삽화)

KISA 망분리 가이드 — *한국의 표준*

📜 근거 법령·고시

- **개인정보보호법** 제29조 (안전성 확보 조치 기준)
- **개인정보의 안전성 확보조치 기준 고시** — 100만명 이상 처리자, 망분리 의무
- **전자금융감독규정** 제15조 — 금융회사 망분리 의무
- **정보통신기반보호법** — 주요정보통신기반시설
- **공공기관 망분리 가이드라인 (KISA)**

🎯 KISA 권고 망분리 5단계

1. 외부 인터넷 차단
2. 외부 메일 서버 분리
3. 업무망 ↔ 인터넷망 물리/논리 분리
4. **망간 자료 전송 통제 시스템** 도입
5. **운영·감사 로그** 보존

📦 망간 자료 전송 시스템 (Data Diode·SecureUSB·NWStat)

- 망간 자료 이동 시 **별도 검역망(Sandbox)** 거쳐 악성코드 차단
- 일방향 게이트웨이 (Data Diode) — 하드웨어 강제 단방향
- 승인 기반 워크플로우
- 국내: 시큐브·소프트캠프·안랩·이니텍·이글로벌시스템

🎙️ TA 메모

- 망분리 설계 = 자료 전송 설계가 절반
- 모든 자료 이동 = 로그 + 감사관 승인

📚 **참조 자료** (공식 가이드·국내 솔루션) - KISA 정보보호 가이드 — KISA 공식 - 개인정보의 안전성 확보조치 기준 (개인정보보호위원회) — 개인정보위 공식 - 전자금융감독규정 (금융위·금감원) — 금융위 공식 - 시큐브 망연계 솔루션 — 시큐브 공식 - 소프트캠프 망간자료전송 — 소프트캠프 공식 - Owl Cyber Defense Data Diode — Owl 공식

DMZ 토폴로지 — *Single · Dual · 3-Tier*

🏰 Single Firewall DMZ

```
Internet – FW (3-leg) ─┬─ DMZ (Web)
                       └─ Internal
```

- FW 1대에 인터넷·DMZ·내부 3개 인터페이스
- 가장 단순·저렴
- FW 1대 침해 = 전체 위험

🏰 Dual Firewall DMZ

```
Internet – FW1 – DMZ – FW2 – Internal
```

- 인터넷↔DMZ는 FW1, DMZ↔내부는 FW2
- **다른 벤더 FW** 권고 — 동일 취약점 회피
- 한국 표준 구성

🏰 3-Tier DMZ

```
Internet – FW1 – Web Tier – FW2 – App Tier – FW3 – DB Tier
```

- 웹·앱·DB 3계층 분리
- 각 계층 사이 FW
- 대형 서비스·금융권

🎙️ TA 결정

- 중소 = Single FW + L7 LB (HTTPS 종단)
- 일반 기업 = **Dual FW** (다른 벤더)
- 금융·대형 공공 = **3-Tier + WAF + IPS**
- DMZ 서버는 **NTP·DNS·로그**만 외부 허용

망간 자료 전송 — *NWStat · SecureUSB · 망연계*

솔루션 종류	동작	사례
망연계 시스템	두 망 사이 게이트웨이로 파일 전송 + 검사	시큐브 SecuwayGate, 소프트캠프 SHIELDEX, 안랩 SafeTransfer
검역망 (Sandbox)	외부에서 들어온 파일 자동 분석	FireEye, Cisco AMP, 안랩 MDS
SecureUSB·세큐어디스크	인가 USB만 사용, 자동 암호화	마크애니, Cyberone
DRM 전송	문서를 DRM으로 포장 전송	마크애니, Fasoo, 소프트캠프
데이터 다이오드	하드웨어 단방향	Owl, Waterfall, 시큐레터
메일 망연계	메일을 망간 전송 전용으로	별도 메일 SMTP 게이트웨이

한국 SI 현장의 통념: 망분리 도입 시 **망연계 시스템이 핵심 SW**. 자료 흐름 통제 + 감사 로그 + 백신 검역 + 승인 워크플로우를 한 솔루션에서.

PART J

SDN · Overlay · SD-WAN · MPLS — *현대 네트워크의 4가지 큰 그림*

> 컨트롤 평면을 분리하고, 가상 네트워크를 오버레이로 띄우고, WAN을 소프트웨어로 제어한다.

SDN — *Software Defined Networking*

🧠 SDN의 핵심

- **Control Plane** (라우팅 결정)과 **Data Plane** (패킷 포워딩) 분리
- 중앙 컨트롤러가 모든 SW에 **일관 정책** 푸시
- 네트워크를 **API로 제어**

🏗️ 표준 프로토콜

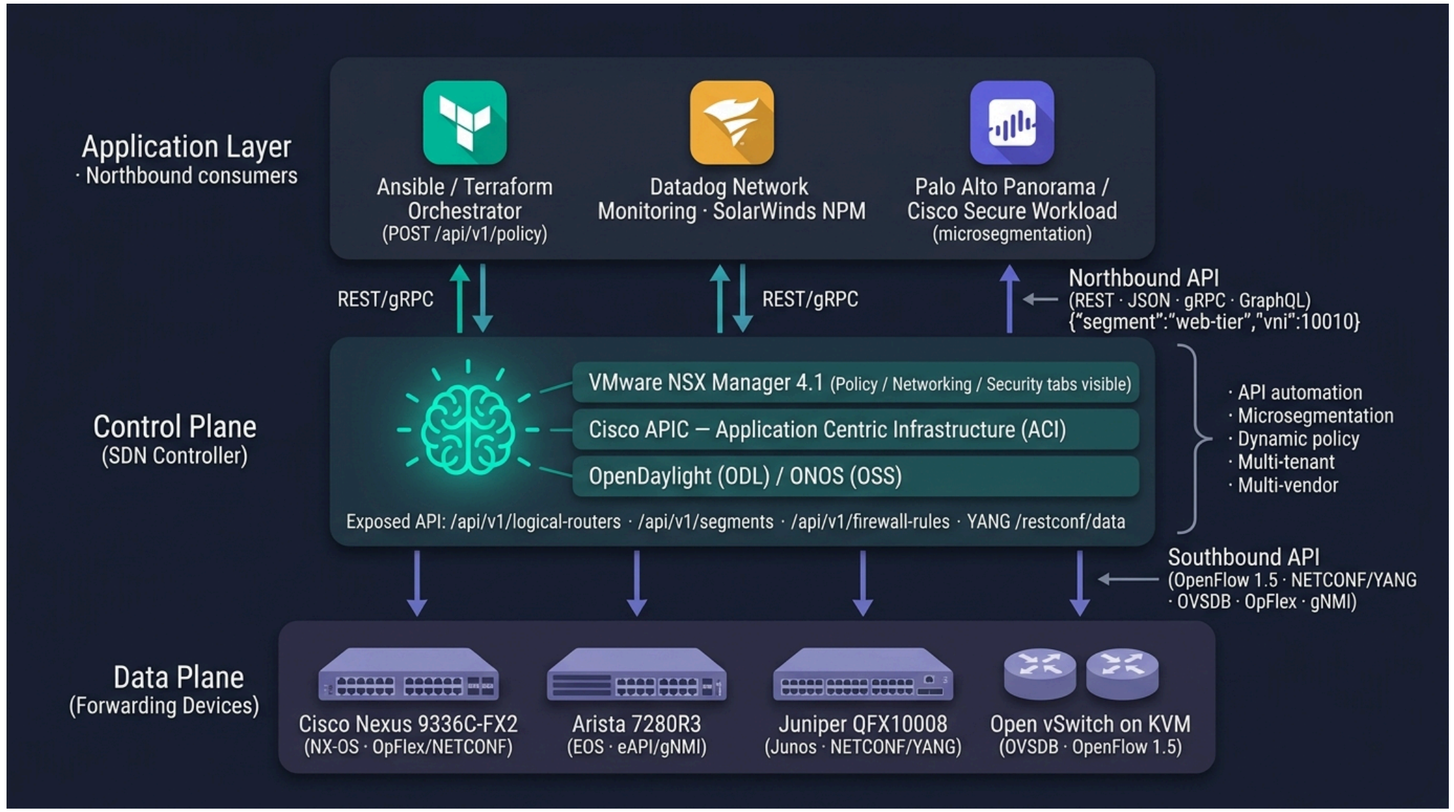
- **OpenFlow** (ONF) — 컨트롤러 ↔ 스위치 표준
- **NETCONF / YANG** — 설정 모델링
- **OpFlex** (Cisco) — ACI 표준
- **OVSDB** — Open vSwitch 관리

🎯 SDN의 장점

- **자동화** — API·CI/CD로 NW 변경
- **마이크로세그멘테이션** — 워크로드 단위 정책
- **동적 변경** — 트래픽·테넌트·앱별 최적화
- 멀티벤더 호환 (이론)

🛠️ 컨트롤러 솔루션

- **VMware NSX** (Network Virtualization) — DC SDN 1위
- **Cisco ACI** (Application Centric Infrastructure)
- **OpenDaylight (ODL)** — OSS 컨트롤러
- **ONOS** — OSS, 통신사 지향
- **Tungsten Fabric (구 OpenContrail)**



SDN 아키텍처 (삽화)

PART K

NMS · 관찰성 — *SNMP · MIB · NetFlow · 솔루션*

> 측정되지 않는 것은 관리되지 않는다. NMS는 NW 운영의 시계·청진기·CCTV.

SNMP — *v1 · v2c · v3 비교*

항목	SNMPv1	SNMPv2c	SNMPv3 ⭐
표준	RFC 1157 (1990)	RFC 1901~ (1993)	RFC 3411~ (2002)
인증	**Community String** (평문)	Community String (평문)	**User-Based (USM)** — Auth + Priv
암호화	❌	❌	**AES-128/192/256**
데이터 타입	기본	+ Counter64 (대역폭)	v2c + 보안
메시지	Get·GetNext·Set·Trap	+ GetBulk·Inform	동일 + 보안
보안 등급	매우 낮음	낮음	**고**
현재 권고	폐기	폐기	**신규 표준**

SNMP v3 보안 모드 — - **noAuthNoPriv**: 인증·암호 모두 없음 - **authNoPriv**: 인증(MD5/SHA) 있고 암호 없음 - **authPriv**: **인증 + 암호 (AES)** — 권장

MIB · OID — *SNMP 데이터 모델*

🗂️ MIB (Management Information Base)

- 장비가 노출하는 **관리 데이터 구조**
- 트리 구조 — 각 노드에 OID 부여
- 표준 MIB + 벤더 MIB

🔢 OID (Object Identifier)

- 점으로 구분된 숫자 시퀀스 (또는 이름)
- 예: `1.3.6.1.2.1.2.2.1.10` = ifInOctets (인터페이스 입력 바이트)
- 예: `1.3.6.1.2.1.2.2.1.16` = ifOutOctets (출력 바이트)

🌳 OID 트리 주요 가지

```
1.3.6.1  iso.org.dod.internet
   .1      directory
   .2      mgmt
     .1      mib-2 (표준 MIB)
       .1      system
       .2      interfaces
       .4      ip
       .6      tcp
       .7      udp
       .25     host
   .4      private
     .1      enterprises
       .9      Cisco
       .2636   Juniper
       .12356  Fortinet
```

🎙️ TA 메모

- 표준 MIB-II로 거의 모든 NMS가 동작
- 벤더 MIB는 CPU·Temp·전원·팬 등 상세 정보

SNMP 동작 — *Get · GetNext · Set · Trap · Inform*

🔄 Polling (NMS → 장비)

- **Get** — 특정 OID 1개 조회
- **GetNext** — 트리 다음 OID
- **GetBulk (v2c+)** — 한 번에 다수 조회 (성능 ↑)
- **Set** — 값 변경 (예: 인터페이스 down)
- 보통 **5~15분 주기 폴링**

📡 Push (장비 → NMS)

- **Trap (v1·v2c·v3)** — 비동기 이벤트 알림
- **Inform (v2c+)** — Trap + ACK (재전송 보장)
- 포트: NMS = **UDP 162**, 폴링은 **UDP 161**

🚨 자주 보는 Trap 종류

- coldStart · warmStart — 장비 부팅
- linkDown · linkUp — 인터페이스 상태
- authenticationFailure — 인증 실패
- 벤더 특정 — Fan·Temp·전원·HA 절체

🎙️ TA 메모

- **Trap은 신뢰성 낮음 (UDP)** — 중요한 이벤트는 Inform 또는 Syslog 병행
- 폴링 주기는 **5분 표준** — 1분은 부하·30분은 너무 늦음
- v3 + Trap 함께 — 보안 + 이벤트

트래픽 분석 — *NetFlow · sFlow · IPFIX 비교*

프로토콜	표준	동작	정확도
NetFlow v5	Cisco 독자 (1996)	**전수 측정** (모든 패킷)	정확, CPU 부담
NetFlow v9	Cisco	템플릿 기반 가변	정확
IPFIX	**IETF RFC 7011**	v9 표준화	정확, 벤더 중립
sFlow	InMon Foundation	**샘플링** (예: 1/1024)	통계적, 저부하
NetStream	Huawei	v5/v9 호환	Cisco 호환

🎯 수집되는 정보 (Flow Record)

- 5-Tuple (Src/Dst IP·Port·Protocol)
- 입·출력 인터페이스 · TCP Flags · DSCP·ToS
- 시작·종료 시간 · 바이트·패킷 수 · AS 번호 (BGP)

한 줄 정리 — IPFIX는 NetFlow v9의 IETF 표준화 버전, sFlow는 샘플링 기반 저부하 솔루션. 운영 활용·샘플링 권고는 다음 페이지에서.

Flow 운영 활용 — *분석 도구 · TA 활용 · 결정 매트릭스*

📊 분석 도구

- **SolarWinds NTA**, **PRTG**, **ManageEngine NetFlow Analyzer**
- OSS: **ntopng**, **Akvorado**, **GoFlow + ClickHouse**
- 통신사: 자체 백엔드 (Kafka + Druid·ClickHouse)

🎙️ TA 활용

- **Top Talkers** — 트래픽 점유 상위
- **이상 트래픽 탐지** — DDoS·내부 봇
- **회선 사용률** — 증설 결정
- **응용별 트래픽** — Office365·SAP·Backup
- **포렌식** — 침해 시 누가 어디로

🎯 결정 매트릭스

구간	권고 프로토콜	샘플링
액세스·캠퍼스 (≤10G)	**NetFlow v9 / IPFIX**	전수
DC 코어 (40G)	IPFIX	1:100~1:1000
DC 스파인·백본 (100G+)	**sFlow** 또는 IPFIX 샘플링	1:1000~1:10000
WAN·인터넷 인입	IPFIX + 자체 백엔드	전수 또는 1:100

⚙️ 운영 권고

- 단일 컬렉터 보다 **NetFlow + sFlow 병행** — 정확도와 처리량의 균형
- TTL 단위로 보관(7일 원본 · 90일 집계 · 1년 KPI) 정책 합의

NMS 대시보드 (삽화)

PART L

산출물·결정·정리 — *오늘 배운 것을 문서로*

> 오늘 다룬 12개 PART를 산출물·결정 매트릭스로 묶는다.

TA의 NW 고급 설계 결정 10가지

#	결정	후보	권고 (전형)
1	게이트웨이 HA	VRRP·HSRP·GLBP	**VRRP (벤더 중립)**
2	스위치 클러스터링	Stack·vPC/MLAG	액세스 = Stack, DC = **vPC/MLAG**
3	DC 백본 토폴로지	3-Tier vs Spine-Leaf	**Spine-Leaf + EVPN-VXLAN**
4	멀티테넌트 격리	VLAN vs VXLAN/EVPN	캠퍼스 = VLAN, DC = **VXLAN (EVPN)**
5	로드 밸런서	F5 vs HAProxy/NGINX vs A10	금융 = **F5**, MSA = HAProxy
6	SSL 처리	Term · Bridge · Pass	일반 = **Term + WAF**
7	DR 자동화	DNS 변경·GSLB	**GSLB (TTL 30s)**
8	망분리 방식	물리 2PC vs VDI	금융 = 물리, 일반 = **VDI**
9	DMZ 토폴로지	Single vs Dual vs 3-Tier	**Dual FW (다른 벤더)**
10	NMS·트래픽 분석	SNMP + NetFlow/sFlow	SNMP v3 + **IPFIX**

네트워크 고급 산출물 — *TA 8종*

📐 도면·표

1. **L2/L3 토폴로지 도면** — Visio/Lucidchart
2. **VLAN 표** — VID·이름·서브넷·GW·용도·담당
3. **IP 주소 계획** (IPAM) — Subnet·할당·예약
4. **MLAG·VRRP 도메인 표** — 페어·Peer Link·VIP

📋 정책·설계서

5. **LB 정책서** — Pool·Member·Health·Persistence
6. **QoS 정책서** — DSCP·CoS·큐 매핑
7. **방화벽·DMZ 도면** + 정책 매트릭스
8. **망분리 도면 + 자료전송 SOP**

📊 운영 산출물

9. **NMS 설계서** — 폴링·임계·알람 매트릭스
10. **장애 대응 SOP** — 시나리오별 절차
11. **변경관리 표준** — 변경 분류·검토·승인·롤백
12. **백업 설정 SOP** — 장비 설정 자동 백업

🎙️ TA 산출물 원칙

- 모든 도면 = **As-Is + To-Be + 마이그레이션** 3장
- 모든 정책 = **신청자·승인자·롤백 책임자** 명시
- **버전 관리** — Git or CMDB
- **반기 정기 갱신**

VLAN 표 산출물 — *예시 템플릿*

VID	이름	서브넷	GW	용도	담당 부서	비고
10	MGT-OOB	10.10.0.0/24	.1	관리망 (OOB)	NW팀	SSH·NMS 전용
20	SVR-WEB	10.20.0.0/24	.1	웹 서비스	운영팀	DMZ
30	SVR-APP	10.30.0.0/24	.1	응용 서비스	운영팀	내부
40	SVR-DB	10.40.0.0/24	.1	DB	DBA팀	내부, 제한 ACL
50	BACKUP	10.50.0.0/24	.1	백업망	운영팀	Jumbo MTU 9000
100	OFFICE-N	192.168.100.0/24	.1	사무 (북관)	인사	사용자망
200	VOICE	192.168.200.0/24	.1	IP 전화	통신팀	LLDP-MED 자동
999	NATIVE-NULL	(사용 안 함)	-	보안용 Native	NW팀	운영 사용 금지

산출물 품질의 척도 — VID·서브넷·게이트웨이만 적힌 표는 "지도", **담당·용도·비고**까지 적힌 표가 "운영 매뉴얼".

LB 정책 산출물 — *예시 템플릿*

서비스	VS IP·Port	Pool 멤버	알고리즘	Health	Persistence	SSL
portal.company.kr	203.0.113.10:443	web01~web04:8080	Least Conn	HTTP /health 5s	Cookie Insert	Term + WAF
api.company.kr	203.0.113.11:443	api01~api04:8080	RR	HTTP /health 5s	None (Stateless)	Term
db-rw.internal	10.40.0.50:5432	pg-master:5432	(단일)	TCP 10s	-	Pass
db-ro.internal	10.40.0.51:5432	pg-replica1~3:5432	Least Conn	TCP 10s	Source IP	Pass
mail.company.kr	203.0.113.20:25	smtp01~smtp02	RR	TCP 30s	None	Pass

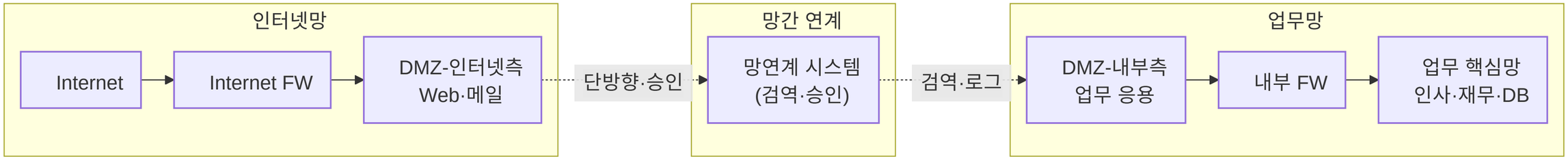
🎯 정책 추가 항목

- **연결 한도** (Connection Limit)
- **세션 타임아웃** (Idle/Long)
- **Rate Limit** (DDoS 완화)
- **로깅 레벨**
- **장애 시 동작** (Drop / Send 503)

🎙️ TA 메모

- **Pool 멤버 수 = N+1 이상**
- 가중치는 사양 비율
- 헬스 체크는 **응용 + DB 점검** 엔드포인트
- SSL 인증서 만료 알람은 NMS·SIEM 연동

망분리 도면·산출물 — *예시 구성*



📐 산출물 5종

- 망분리 도면 (As-Is·To-Be)
- 자료 전송 SOP — 신청·검토·승인·기록
- 검역 정책 — 백신·샌드박스·콘텐츠 검사
- 사용자 가이드 — 메일·파일 전송 절차
- 감사 로그 보존 정책 — 3년 이상

🎙️ TA 메모

- 망연계는 **단방향 + 승인 + 로그** 3종 세트
- 사용자 경험 = 절차 단순화 + 자동화
- 모의 침투·정기 감사 필수

한국 현장 토픽 — *체크리스트*

🇰🇷 한국 SI 특수성

- **망분리 의무** — KISA·금감원·개정법 매년 점검
- **공인 인증서·KISA 인증 솔루션** 우선
- **이중화·HA 강조** — N+1 기본
- **국산 솔루션 가산점** — NMS·LB·망연계
- **공공 = 단방향 게이트웨이** 사례 다수
- **금융 = 물리 2PC + DRM** 표준

🛒 벤더 매트릭스 (현장 친숙도)

- LB = **F5 압도적**, A10·HAProxy 증가
- NMS = SolarWinds + 국산 (다산데이타·VCNC·다인스)
- 망연계 = 시큐브·소프트캠프·안랩·이니텍

📋 RFP·제안 시 자주 묻는 표준

- ISMS-P 적합성
- CC 인증 / 보안기능 확인서
- KCMVP 암호 모듈
- IPv6 지원 (의무화)
- BGP·OSPF 라우팅 자격
- GSLB 동시 다중 사이트
- 망분리·DMZ 도면 + 자료 전송 정책

🎙️ TA 메모

- 한국 사업의 90%는 위 체크리스트 안에서 답을 찾는다
- 신규 사업도 **레거시 호환**을 함께 다룬다 (혼합 운영 가이드)

핵심 키워드 — *시험·면접 대비*

A·C·D

- 802.1Q · Native VLAN
- Trunk · Access
- Private VLAN (Isolated·Community)
- Voice VLAN
- VLAN Hopping · DTP
- STP · RSTP · MSTP
- BPDU/Root/Loop Guard
- Stack · vPC · MLAG
- VRRP · HSRP · GLBP · CARP
- ECMP · Per-Flow Hash

E·F·G·H

- Static NAT · PAT · Hairpin
- NAT64 · DNS64
- STUN · TURN · ICE
- DSCP · CoS · EF · AF
- LLQ · CBWFQ
- Policing vs Shaping
- L4 vs L7 LB
- Least Conn · Source Hash
- SSL Termination · Bridging · Pass-through
- Active vs Passive Health
- Cookie Persistence
- GSLB · Active-Active · DR Failover
- DHCP DORA · Option 82
- IPv6 SLAAC · Dual-Stack

I·J·K

- 물리 망분리 · 논리 망분리
- VDI · SBC · CBC
- KISA 가이드
- DMZ Single/Dual/3-Tier
- 망연계 시스템
- SDN · OpenFlow · NETCONF
- VMware NSX · Cisco ACI
- VXLAN · VNI · VTEP
- EVPN-VXLAN
- SD-WAN
- SNMP v3 · MIB · OID
- NetFlow · sFlow · IPFIX
- Trap · Inform